CLAIMS

What is claimed is:

1. A method for performing authentication operations, the method comprising:

performing a non-certificate-based authentication operation through an SSL (Secure Sockets Layer) session between a server and a client; and

subsequent to performing the non-certificate-based authentication operation, performing a certificate-based authentication operation through the SSL session between the server and the client without exiting or renegotiating the SSL session prior to completion of the certificate-based authentication operation.

2. The method of claim 1 wherein negotiation of the SSL session uses a first digital certificate from the client, wherein the certificate-based authentication operation uses a second digital certificate from the client, and wherein the first digital certificate and the second digital certificate are not identical.

3. The method of claim 1 further comprising:

providing access to a first resource for a client by a server in association with the non-certificate-based authentication operation.

4. The method of claim 3 wherein the step of providing access to the first resource further comprises:

receiving at the server a first resource request from the client;

in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request, establishing an SSL (Secure Sockets Layer) session between the server and the client; and

in response to successfully performing the non-certificate-based authentication operation between the server and the client through the SSL session, sending a first resource response from the server to the client.

5. The method of claim 1 further comprising:

providing access to a second resource for a client by a server in association with the certificate-based authentication operation.

6. The method of claim 5 wherein the step of providing access for the second resource further comprises:

receiving at the server a second resource request from the client through the SSL session;

in response to determining that the second resource request requires a certificate-based authentication procedure, downloading an executable module to the client from the server through the SSL session;

receiving at the server a digital signature that has been generated by the executable module using a digital certificate at the client; and

in response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client.

7. The method of claim 5 wherein the step of providing access for the second resource further comprises:

receiving at the server a second resource request from the client through the SSL session;

in response to determining that the second resource request requires a certificate-based authentication procedure, triggering execution of a downloadable software module at the client by the server through the SSL session;

receiving at the server a digital signature that has been generated by the execution of the downloadable software module using a digital certificate at the client; and

in response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client.

8. The method of claim 1 further comprising:

obtaining access to a second resource at a server by a client in association with the certificate-based authentication operation.

9. The method of claim 8 wherein the step of obtaining access to the second resource further comprises:

sending a second resource request from the client to the server through the SSL session;

receiving an executable module at the client from the server through the SSL session, wherein the executable module comprises functionality for performing a certificate-based authentication operation;

sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

receiving a second resource response from the server at the client.

10. The method of claim 8 wherein the step of obtaining access to the second resource further comprises:

sending a second resource request from the client to the server through the SSL session;

receiving at the client from the server through the SSL session a response message having content with an associated content type indicator;

in response to determining a content type for the content, executing a downloadable software module at the client;

sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

receiving a second resource response from the server at the client.

11. An apparatus for performing authentication operations, the apparatus comprising:

means for performing a non-certificate-based authentication operation through an SSL (Secure Sockets Layer) session between a server and a client; and

means for performing, subsequent to performing the non-certificate-based authentication operation, a certificate-based authentication operation through the SSL session between the server and the client without exiting or renegotiating the SSL session prior to completion of the certificate-based authentication operation.

12. The apparatus of claim 11 wherein negotiation of the SSL session uses a first digital certificate from the client, wherein the certificate-based authentication operation uses a second digital certificate from the client, and wherein the first digital certificate and the second digital certificate are not identical.

13. The apparatus of claim 11 further comprising:

means for providing access to a first resource for a client by a server in association with the non-certificate-based authentication operation.

14. The apparatus of claim 13 wherein the means for providing access to the first resource further comprises:

means for receiving at the server a first resource request from the client;

means for establishing an SSL (Secure Sockets Layer) session between the server and the client in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request; and

means for sending a first resource response from the server to the client in response to successfully performing the non-certificate-based authentication operation between the server and the client through the SSL session.

15. The apparatus of claim 11 further comprising:

means for providing access to a second resource for a client by a server in association with the certificate-based authentication operation.

16. The apparatus of claim 15 wherein the means for providing access for the second resource further comprises:

means for receiving at the server a second resource request from the client through the SSL session;

means for downloading an executable module to the client from the server through the SSL session in response to determining that the second resource request requires a certificate-based authentication procedure;

means for receiving at the server a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.

17. The apparatus of claim 15 wherein the means for providing access for the second resource further comprises:

means for receiving at the server a second resource request from the client through the SSL session;

means for triggering execution of a downloadable software module at the client by the server through the SSL session in response to determining that the second resource request requires a certificate-based authentication procedure;

means for receiving at the server a digital signature that has been generated by the execution of the downloadable software module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.

18. The apparatus of claim 11 further comprising:

means for obtaining access to a second resource at a server by a client in association with the certificate-based authentication operation.

19. The apparatus of claim 18 wherein the means for obtaining access to the second resource further comprises:

means for sending a second resource request from the client to the server through the SSL session;

means for receiving an executable module at the client from the server through the SSL session, wherein the executable module comprises functionality for performing a certificate-based authentication operation;

means for sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for receiving a second resource response from the server at the client.

20. The apparatus of claim 18 wherein the means for obtaining access to the second resource further comprises:

means for sending a second resource request from the client to the server through the SSL session;

means for receiving at the client from the server through the SSL session a response message having content with an associated content type indicator;

means for executing a downloadable software module at the client in response to determining a content type for the content;

means for sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for receiving a second resource response from the server at the client.

21. A computer program product in a computer-readable medium for use in a data processing system for performing authentication operations, the computer program product comprising:

means for performing a non-certificate-based authentication operation through an SSL (Secure Sockets Layer) session between a server and a client; and

means for performing, subsequent to performing the non-certificate-based authentication operation, a certificate-based authentication operation through the SSL session between the server and the client without exiting or renegotiating the SSL session prior to completion of the certificate-based authentication operation.

22. The computer program product of claim 21 wherein negotiation of the SSL session uses a first digital certificate from the client, wherein the certificate-based authentication operation uses a second digital certificate from the client, and wherein the first digital certificate and the second digital certificate are not identical.

23. The computer program product of claim 21 further comprising:

means for providing access to a first resource for a client by a server in association with the non-certificate-based authentication operation.

24. The computer program product of claim 23 wherein the means for providing access to the first resource further comprises:

means for receiving at the server a first resource request from the client;

means for establishing an SSL (Secure Sockets Layer) session between the server and the client in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request; and

means for sending a first resource response from the server to the client in response to successfully performing the non-certificate-based authentication operation between the server and the client through the SSL session.

25. The computer program product of claim 21 further comprising:

means for providing access to a second resource for a client by a server in association with the certificate-based authentication operation.

26. The computer program product of claim 25 wherein the means for providing access for the second resource further comprises:

means for receiving at the server a second resource request from the client through the SSL session;

means for downloading an executable module to the client from the server through the SSL session in response to determining that the second resource request requires a certificate-based authentication procedure;

means for receiving at the server a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.

27. The computer program product of claim 25 wherein the means for providing access for the second resource further comprises:

means for receiving at the server a second resource request from the client through the SSL session;

means for triggering execution of a downloadable software module at the client by the server through the SSL session in response to determining that the second resource request requires a certificate-based authentication procedure;

means for receiving at the server a digital signature that has been generated by the execution of the downloadable software module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.

28. The computer program product of claim 21 further comprising:

means for obtaining access to a second resource at a server by a client in association with the certificate-based authentication operation.

29. The computer program product of claim 28 wherein the means for obtaining access to the second resource further comprises:

means for sending a second resource request from the client to the server through the SSL session;

means for receiving an executable module at the client from the server through the SSL session, wherein the executable module comprises functionality for performing a certificate-based authentication operation;

means for sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for receiving a second resource response from the server at the client.

30. The computer program product of claim 28 wherein the means for obtaining access to the second resource further comprises:

means for sending a second resource request from the client to the server through the SSL session;

means for receiving at the client from the server through the SSL session a response message having content with an associated content type indicator;

means for executing a downloadable software module at the client in response to determining a content type for the content;

means for sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for receiving a second resource response from the server at the client.

31. A method for performing authentication operations, the method comprising:

receiving at a server a first resource request from a client;

in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request, establishing an SSL (Secure Sockets Layer) session between the server and the client;

performing a non-certificate-based authentication operation through the SSL session;

in response to successfully performing the non-certificate-based authentication operation, sending a first resource response from the server to the client;

receiving at the server a second resource request from the client through the SSL session subsequent to performing the non-certificate-based authentication operation;

in response to determining that the second resource request requires a certificate-based authentication procedure, downloading an executable module to the client from the server through the SSL session;

receiving at the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

in response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client.

32. An apparatus for performing authentication operations, the apparatus comprising:

means for receiving at a server a first resource request from a client;

means for establishing an SSL (Secure Sockets Layer) session between the server and the client in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request;

means for performing a non-certificate-based authentication operation through the SSL session;

means for sending a first resource response from the server to the client in response to successfully performing the non-certificate-based authentication operation;

means for receiving at the server a second resource request from the client through the SSL session subsequent to performing the non-certificate-based authentication operation;

means for downloading an executable module to the client from the server through the SSL session in response to successfully performing the non-certificate-based authentication operation;

means for receiving at the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.

33. A computer program product in a computer-readable medium for use in a data processing system for performing authentication operations, the computer program product comprising:

means for receiving at a server a first resource request from a client;

means for establishing an SSL (Secure Sockets Layer) session between the server and the client in response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request;

means for performing a non-certificate-based authentication operation through the SSL session;

means for sending a first resource response from the server to the client in response to successfully performing the non-certificate-based authentication operation;

means for receiving at the server a second resource request from the client through the SSL session subsequent to performing the non-certificate-based authentication operation;

means for downloading an executable module to the client from the server through the SSL session in response to successfully performing the non-certificate-based authentication operation;

means for receiving at the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and

means for sending a second resource response from the server to the client in response to successfully verifying the digital signature at the server.